POLICIES AND OPERATING PROCEDURES USED TO ENSURE COMPLIANCE WITH FCC RULES REGARDING CPNI

1. FOREMOST TELECOMMUNICATIONS CORPORATION (d/b/a FOREMOST TELECOMMUNICATIONS, hereinafter "FOREMOST") as a matter of policy does not make Customer Proprietary Network Information (hereinafter "CPNI") available to any third-party except as necessary to provide service, to comply with applicable interconnection agreements and inter-carrier requirements, and as routinely disclosed at the signaling layer.

2. As CPNI is not disclosed to third-parties except as provided above, FOREMOST is not required to provide its customers with a notice or a mechanism to opt out of the use of their CPNI by third-parties. Any changes to this policy allowing such disclosure to third-parties shall require the adoption of a notice to the customer, a mechanism for the customer to opt out of such disclosure, and status reporting, all in accord with 47 C.F.R. §64.2001, *et seq.*

3. FOREMOST does not use CPNI for external sales or marketing campaigns. Further, FOREMOST personnel are not authorized to conduct any sales or marketing efforts which use CPNI, and do not have access to systems where CPNI is stored and maintained. Any changes or exceptions to this policy may require record-keeping and a supervisory review process as required by 47 C.F.R. §64.2001, *et seq*. The President of FOREMOST may direct and supervise internal sales efforts that may use CPNI on a case-by-case basis to provide or market service offerings among the categories of service to which an existing FOREMOST customer already subscribes (e.g. contract renewals), and all such activity is required to be recorded and maintained in accord with 47 C.F.R. §64.2001, *et seq*.

4. All FOREMOST personnel are trained that CPNI may only be used for allowed purposes, as narrowly defined herein, and are aware that the unauthorized use of CPNI shall be grounds for dismissal. All personnel are required to review and sign training documents defining CPNI, the appropriate procedures to ensure compliance, and the disciplinary process that shall be undertaken for failure to comply with CPNI rules.

5. CPNI is protected from unauthorized access and use. Systems that are used to store and maintain CPNI are firewalled from the public internet and data is protected at the network level using VPN technology. Only information associated with individual login sessions is stored on workstations and all data repositories are centralized on servers. Data is segregated at the server level, such that FOREMOST personnel who do not have access to CPNI also do not have accounts on servers where CPNI is stored. Backups are encrypted with password protection. Login credentials are controlled and are changed periodically. Hardcopies are not produced except in a directed manner, such as for a particular customer for an authorized use. Hardcopies produced for temporary use (e.g., installation and maintenance activities) are destroyed after use.

6. Supervisory review at the highest level exists to ensure the foregoing policies and procedures are followed.

7. FOREMOST does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.